UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

UNITED STATES OF AMERICA	)	
	)	**No. 3:24-CR-00151**
v.	)	**JUDGE RICHARDSON**
	)	
MATTHEW ISSAC KNOOT	)	

REPLY SUPPORTING MOTION TO SUPPRESS

The Government seized and searched Matthew Knoot's personal desktop computer and cellphone pursuant to a defective warrant and then used information discovered on that desktop and cellphone to compel Discord, Inc. to disclose (to the Government) communications between two Discord users (one with username "mellamomateao"; the other, "yandgi0027").

Under these circumstances, this Court should—at the very least—suppress: (1) any information law enforcement obtained from Knoot's personal devices (i.e., his personal desktop computer and cellphone), and (2) the Discord communications between "mellamomateao" and "yandgi0027" (because the Government used tainted information to obtain them).

Hoping to save the fruits of the search of Knoot's personal devices from exclusion, the Government claims: (1) that the Device Warrant validly authorized it to search those devices, (2) that Knoot lacks standing to challenge the admissibility of the Discord communications, and (3) that, in any event, suppression is unwarranted because law enforcement acted in good faith.[1]

These arguments are unpersuasive, so this Court should reject them, grant Knoot's Motion to Suppress (DE 48), and suppress the Discord communications and any information law enforcement obtained from their search of Knoot's personal devices.

[1] The Government also argues that the Device Warrant (which the Government calls the "Premises Warrant") and the Discord Warrants are sufficiently particularized and not overbroad. Knoot disagrees for the reasons outlined in his opening motion, but, for the sake of brevity, focuses in this reply on the nexus, standing, and good-faith issues.

1. The affidavit submitted in support of the Device Warrant does not establish a nexus between the crimes under investigation and Knoot's personal devices.

One problem with the Device Warrant is that it authorized agents to search Knoot's personal devices even though the affidavit that Agent Rousseau submitted in support of it relied solely on training-and-experience allegations (as opposed to case-specific facts) to draw a nexus between those devices and the crimes under investigation. (DE 48, Mot., PageID #129-134).

Why is this a problem? It's because a warrant cannot validly authorize the search of a device unless the affidavit submitted in support of it establishes that the device was used "in connection with criminal activity." *United States v. Powell*, 943 F. Supp. 2d 759, 779 (E.D. Mich. 2013), *aff'd*, 847 F.3d 760 (6th Cir. 2017); *see also United States v. Bass*, 785 F.3d 1043, 1049 (6th Cir. 2015) (nexus established when "affidavit stated" that defendant used device in furtherance of crime); *see also United States v. Brown*, 828 F.3d 375, 382 (6th Cir. 2016) (generally discussing nexus requirement). And since *Schultz* provides that an officer's training-and-experience allegations cannot alone satisfy the Fourth Amendment's nexus requirement, *United States v. Schultz*, 14 F.3d 1093, 1097 (6th Cir. 1994), the Device Warrant is invalid insofar as it authorized a search Knoot's personal devices, (*see* DE 48, Mot., PageID #130-32).

Seeking to avoid the result that *Schultz* commands (suppression of the fruits of the search of Knoot's personal devices), the Government makes three assertions. None have merit.

a. First, the Government seems to suggest that, because the warrant affidavit established a case-specific nexus between the crimes under investigation and Knoot's apartment and/or the victim laptops, it did not need to establish a *separate* nexus between those crimes and Knoot's personal devices. (DE 52, Gov't Resp., PageID #262 (claiming that "the distinction between a 'victim' laptop and a 'personal' [device] is unwarranted"), #263 (contending that the affidavit

articulated "a clear and specific nexus between the crimes under investigation and the defendant's home" and suggesting that this is sufficient to connect Knoot's personal devices to the crime).

That is incorrect. Knoot's personal devices are "places" or "things" that are capable of being searched in their own right. *See Riley v. California*, 573 U.S. 373 (2014) (officers generally need a warrant to search a device, even when the device is seized incident to arrest).

To that end, the fact that the affidavit established a factual nexus between the crimes under investigation and *other* "places" or "things" to be searched (such as Knoot's residence and the victim laptops) is largely beside the point. Instead, to validly authorize the search of Knoot's personal desktop computer and cellphone, the affidavit needed to include case-specific facts connecting those specific devices to the suspected criminal activity. *See, e.g.*, *Bass*, 785 F.3d at 1049 (warrant authorizing search of device was valid because it stated facts connecting the device to a crime); *Powell*, 943 F. Supp. at 778 (requiring government to draw a concrete factual nexus between the "specific cell phone" that it wanted to search and the crimes under investigation).

b. Second, and perhaps realizing that Agent Rousseau's "training and experience" allegations (¶¶ 26, 27) do not by themselves establish a nexus between the crimes under investigation and Knoot's personal devices, the Government suggests that ¶ 17 and ¶ 20 of the affidavit imply that Knoot's devices *must* have somehow been used to facilitate crime. Not so.

Consider ¶ 17 first. All that paragraph says is that "Victim 1 reported that [A.M.], while working with his company-issued laptop, [used] a [VPN] to connect to Chinese [IP] addresses." (DE 50-1, ¶ 17). It says nothing about Knoot's personal devices, much less whether or how those devices were used in connection with the crimes under investigation. Nor does the allegation in ¶ 17 "indicate[]" that a co-conspirator "located somewhere other than Nashville" was accessing

Victim 1's laptop.[2] (DE 52, Gov't Resp., PageID #265). Quite the contrary, the affidavit expressly provides that, "[a]s it relates to this application," a VPN "can . . . be used to . . . make Internet traffic appear as if [it's] coming from another location." (DE 50-1, ¶ 15). And if anything, this attestation shows that law enforcement believed a single person was using a VPN on Victim 1's laptop to make it appear as though he or she was somewhere other than he actually was—not that that person was using a VPN to allow a third-party to remotely access Victim 1's laptop.[3]

To that end, and contrary to the Government's argument, ¶ 17 does not include "specific and concrete" facts (as opposed to "vague" and "generalized" assertions) indicating that Knoot's personal devices were somehow used in connection with the crimes under investigation.

Next, ¶ 20. This paragraph explains that, in addition to Victim 1, at least two more domestic companies—referred to as Victims 2 and 3—shipped laptops to Knoot's apartment "after hiring an individual they believed was" A.M. (DE 50-1, ¶ 20). Like ¶ 17, this paragraph says nothing about Knoot's personal desktop or cellphone and certainly doesn't specifically say that he used his desktop or cellphone to facilitate the commission of the crimes being investigated.

Reading between the lines, the Government says that this paragraph shows that Knoot *must* have used his personal devices to apply for these jobs or to "communicate with someone to get Victim 1 to ship a laptop to his home." (DE 52, Gov't Resp., PageID #263).

---

[2] The Government suggests that ¶ 17 establishes Agent Rosseau knew that the crimes under investigation involved at least two actors and that, consequently, law enforcement needed to search Knoot's personal devices for co-conspirator communications. But that's not what ¶ 17 actually says. And, in context, it's not what ¶ 17 implies. Moreover, even if ¶ 17 vaguely implies the existence of a co-conspirator, the affidavit still lacks concrete, case-specific facts showing that Knoot used his personal devices to communicate with that co-conspirator. *Cf. Bass*, 783 F.3d at 1049 (finding nexus between defendant's cell phone and crimes under investigation because "the affidavit stated that [the defendant] and his co-conspirators frequently used cell phones to communicate").

[3] For a basic overview of how VPNs work, see Yuliana Reyes, *Anonymous & Unregulated: Why A Product of Privacy Needs Regulation*, 48 Nova L. Rev. 192, 195 (2024).

But that's not necessarily true. Job applications are not always electronic (and the affidavit does not suggest that the job applications submitted to Victims 1, 2, or 3 were submitted on the Internet). And even when they are, applicants often use resources available at the public library to complete and submit them. *Job Search Resources*, Nashville Public Library, *available at* https://www.ala.org/sites/default/files/aboutala/content/publishing/editions/webextras/jerrard10139/Web%20Extra/tips_using_computers.pdf (last visited Apr. 25, 2025).

Further, and perhaps more importantly, the four corners of the affidavit do not actually say that Knoot used his personal devices to apply for these jobs or to communicate with co-conspirators—there's no concrete *facts* supporting those theories. *Brown*, 828 F.3d at 382.

That's problematic. When determining whether a warrant affidavit establishes a nexus between a crime under investigation and a place or item to be searched, "the reviewing court is concerned *exclusively* with the statements contained within the affidavit itself." *United States v. Weaver*, 99 F.3d 1372, 1378 (6th Cir. 1996) (emphasis added). Although those statements are not interpreted hyper-technically, it's nonetheless "imperative that affidavit accurately reflect the facts of a particular situation" and include case-specific information—as opposed to "generalized boilerplate recitations"—clearly demonstrating a nexus between the place or thing to be searched and the crimes under investigation. *Id.*; *see also Brown*, 828 F.3d at 382 (discussing nexus)

Here, at bottom, the affidavit lacks case-specific facts—and doesn't really even include "vague" and "generalized" facts—establishing how Knoot's personal devices were used "in connection with criminal activity." *Powell*, 943 F. Supp. at 779. Thus, the Device Warrant is invalid insofar as it authorized the search of Knoot's personal desktop and cellphone.

c. Third, the Government suggests that, even if the affidavit lacks concrete nexus-establishing facts, a nexus exists because "[i]t is reasonable to infer that evidence related to

computer fraud and identity theft" (i.e., the crimes under investigation) "would be found . . . on [Knoot's personal] digital devices." (DE 52, Gov't Resp., PageID #261). That is incorrect.

Although it's true that "whether a sufficient nexus has been shown to a particular location turns in part on the type of crime being investigated," (*see id.*, PageID #259 (citation omitted)), it does not follow from that proposition that certain places and items are always subject to search and seizure as long as the substantive crime under investigation is of a particular variety.

Quite the contrary, whether a nexus exists between an item to be searched and a suspected crime is always "a fact-intensive question," *Brown*, 828 F.3d at 382—hence, the Government cannot infer a nexus simply by reference to the type of crime under investigation, *see Weaver*, 99 F.3d at 1378 (explaining that, if law enforcement could establish a nexus with "generalized boilerplate recitations designed to meet all law enforcement needs for . . . certain types of criminal conduct," the warrant's nexus and particularity requirements would be toothless).

And even if it could, no such inference is warranted here. At the time Agent Rosseau prepared the warrant affidavit, agents were investigating Knoot for computer fraud and knew that three companies had shipped laptops to Knoot's apartment under (what appeared to be) false pretenses. (DE 50-1, pg. 3, ¶¶ 17, 20). Under those facts, law enforcement knew *exactly* what they were looking for: three *laptops* that had been shipped to Knoot's apartment and allegedly accessed without authorization. Why law enforcement also thought Knoot's personal desktop computer and cellphone were instrumentalities or evidence computer fraud is unclear, and that's why Agent Rosseau needed to include facts in his affidavit showing a connection between that crime and those devices. But he didn't. Agents were also investigating identity theft. Unlike computer fraud, identity theft does not necessarily involve the use of an electronic device—indeed, as the Supreme Court has observed, "dumpster diving" and "stealing paperwork" (neither of which

require Internet access) are "classic" examples of identity theft. *Flores-Figueroa v. United States*, 556 U.S. 646, 656 (2009). So again, if Agent Rosseau had facts showing that Knoot's personal devices were involved in the commission of identity theft, he needed to include those facts in the affidavit. He did not do so. The result is that the required nexus is missing.

All that said, the Government is asking this Court to hold that officers can obtain a valid warrant to search every inch of data on a defendant's personal digital devices as long as an officer has said in the warrant's supporting affidavit that his training has taught him that "[i]ndividuals who engage in criminal activity . . . use digital devices" to do so. (DE 50-1, ¶ 26).

Since this is precisely the sort of vague and generalized allegation that *cannot* be used to satisfy the Fourth Amendment's nexus requirement, this Court should find that the officers violated the Fourth Amendment when they searched Knoot's personal devices.

2. Knoot has a reasonable expectation of privacy in the Discord communications.

Because the affidavit submitted in support of the Device Warrant failed to establish a nexus between Knoot's personal devices and the crimes under investigation, the search of those devices violated the Fourth Amendment, and any information obtained from those devices is tainted.

This presents a problem for the Discord Warrants. Law enforcement cannot use tainted information to obtain a warrant. *United States v. Smith*, 730 F.2d 1052, 1056 (6th Cir. 1984). Yet that's exactly what they did: they illegally searched Knoot's personal desktop computer, found documents containing excerpts from what "appeared to be partial conversations" between two Discord users—namely, "mellamomateao" and "yangdi0027"—and then used those tainted excerpts to get warrants compelling Discord to produce (among other things) any and all stored communications between those two users. (DE 48, Mot., PageID #135-36).

Notably, the Government does not appear to dispute the proposition that, *if* the information obtained from Knoot's personal devices is tainted, then so too are the fruits of the Discord Warrants—including the communications between "mellamomateao" and "yangdi0027."

Instead, it claims that, insofar as Discord extracted those communications from the *yangdi0027* Discord account as opposed to the *mellamomateao* account, Knoot lacks standing to challenge their admissibility. (DE 52, Gov't Resp., PageID #267-68). That is incorrect.

"The question of whether a defendant has 'standing' to challenge an allegedly illegal search collapses into the substantive issue of whether the defendant had" either "a legitimate expectation of privacy" or a common-law property interest in the place or item searched. *United States v. King*, 227 F.3d 732, 743 n.1 (6th Cir. 2000); *see also United States v. Russell*, 26 F.4th 371, 374 (6th Cir. 2022) (explaining that "[c]ourts using 'standing' as a 'shorthand'" in the Fourth Amendment context to refer to the concept that a defendant must have an interest in the place searched); *Carpenter v. United States*, 585 U.S. 296, 399 (2018) (Gorsuch, J., dissenting) (relying on common-law property concepts analyze defendant's Fourth Amendment rights in data).

Thus, the pertinent question is whether Knoot has a legitimate expectation of privacy (or some other interest) in the communications he sent and received on Discord, regardless of which specific Discord account those communications are extracted from. The answer is yes.

The Sixth Circuit has held "that individuals generally have reasonable expectations of privacy in the [contents] of emails that they send through commercial providers[.]" *See, e.g.*, *United States v. Miller*, 982 F.3d 412, 426 (6th Cir. 2020); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (holding that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through" an Internet provider).

And surely that expectation extends beyond emails to *other* types of electronic communications—like the instant messages that Discord users send and receive via the Discord app. After all, like email, instant messaging "plays an indispensable part in the Information Age," and thus (like email) should receive "strong protection under the Fourth Amendment." *Warshak*, 631 F.3d at 288; Youngjin Choi, *Mobile Instant Messaging Evidence in Criminal Trials*, 26 Cath. U.J.L. & Tech. 1 (2017) (noting that "[a] marketing research firm predicated that by the year 2019, more than 2.19 billion people will use" instant messaging apps "worldwide"). Plus, as Discord's privacy policy shows, Discord vigorously protects the data and communications of its users. *See* Discord Privacy Policy, *available at* https://discord.com/privacy (last visited April 26, 2025).

Knoot also has a common-law property interest in the communications he sent or received via Discord. As Justice Gorsuch explained in his *Carpenter* dissent, common-law property concepts—such as the rules of bailment—show that "the fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them." *Carpenter*, 585 U.S. at 399 (Gorsuch, J., dissenting). And since Knoot's communications on Discord can easily be likened to his "papers" or "effects," it stands to reason that the fact Discord (a communication intermediary) and/or yangdi0027 (another Discord user) had access to those communications does not preclude him from challenging the *Government*'s ability to access them.

In this way, it was reasonable for Knoot to expect that any communications he sent or received via Discord would not be disclosed to law enforcement absent a valid warrant.

It also does not matter that Discord may have located the stored communications between mellamomateao and yangdi0027 by reference to the *yangdi0027* account as opposed to Knoot's account (*mellamomateao*). (DE 50-2, ¶ 1). The Government directed the Discord Warrants to Discord, a communication intermediary. Since a "subscriber" to (or user of) an "intermediary that

makes" electronic communication "possible" has a Fourth Amendment interest "in the contents of" communications that he sends or receives through that intermediary and which are then stored on that intermediary's servers, *Warshak*, 631 F.3d at 286-88, Knoot has a Fourth Amendment interest in his Discord communications regardless whether those communications are deemed to be associated with the yangdi0027 account or the mellamomateao account. To hold otherwise would effectively permit "[t]he protections of the Fourth Amendment" to "turn on" a "coincidence"—namely, the coincidence of *how* Discord goes about locating or producing the stored communications—and, as the Supreme Court has explained, the Fourth Amendment does not work that way. *See California v. Acevedo*, 500 U.S. 565 (1991).

All that said, Knoot has a Fourth Amendment interest in the communications that he sent or received via Discord and which are stored on Discord's servers, and that interest persists regardless which account Discord uses to locate those communications. The result? Knoot has standing to seek suppression of the communications Knoot sent or received via Discord.

3. The good faith exception to the exclusionary rule is inapplicable.

Last, the Government says that, regardless whether law enforcement violated the Fourth Amendment by searching Knoot's personal devices (and then violated those rights again by using information obtained from those devices to compel Discord to produce certain communications), this Court should nonetheless allow it to use the fruits of these searches against Knoot at trial. (DE 52, Gov't Resp., PageID #268-70). This is because (the Government contends), to the extent law enforcement violated Knoot's Fourth Amendments rights, they did so in "good faith." (*Id.*).

That is incorrect. "When evidence is obtained in violation of the Fourth Amendment," the "exclusionary rule usually precludes its use in a criminal proceeding." *Illinois v. Krull*, 480 U.S. 340 (1987). In *Leon*, however, the Supreme Court "created the so-called 'good faith' exception"

to the general rule of exclusion. *United States v. Ward*, 967 F.3d 550, 554 (6th Cir. 2020). Under it, the Government bears the burden of showing that law enforcement obtained the evidence in question in "reasonable, good-faith reliance on a" defective search warrant. *Id.* (citation omitted); Tracey Bateman, et al., *Federal Procedure*, § 33:635 ("[T]he government bears the burden of demonstrating that . . . law enforcement['s] [conduct] satisfie[s]" the good-faith exception). If the Government meets this burden, the evidence is saved.[4] *Ward*, 967 F.3d at 554.

Pertinent here, one way the Government can satisfy the good faith exception is by showing that the affidavit which produced the defective warrant was not "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Id.* (citation omitted).

But, generally speaking, a warrant *is* "so lacking in indicia of probable cause" if it: (1) states only "suspicions, or conclusions, without providing some underlying factual circumstances," or (2) fails to make "*some* connection between the illegal activity and the place to be searched." *Id.* (internal quotation marks and citation omitted) (emphasis in original).

With that framework in mind, has the Government shown that Agent Rosseau's warrant affidavit draws "*some* connection" between "illegal activity" and Knoot's personal devices? *Id.*

The answer is no. The affidavit does include any facts (expressly or implicitly) suggesting that Knoot's personal devices were somehow involved in the crimes under investigation. Instead, Agent Rosseau simply "conclu[ded]" (or really, *assumed*) that they were because his training and experience has taught him that "[i]ndividuals who engage in criminal activity . . . use digital devices" to facilitate their crimes. (DE 50-1, ¶ 26). In this way, the affidavit not only fails to

[4] The Government faults Knoot for not addressing the good-faith doctrine in his opening motion, (*see* DE 52, Gov't Resp., PageID #270)—but, given that that doctrine is an exception to the exclusionary rule, the Government bears the burden of proving its applicability, *see, e.g.*, *United States v. Gregory*, 497 F. Supp. 3d 243, 279 (E.D. Ky. 2020) ("The burden is on the government to show that suppression is inappropriate" by invoking "one of the" exclusionary rule's "exceptions."). In this way, Knoot did not need to address this exception in his opening motion, nor does he otherwise bear any burden with respect to its application.

establish a nexus between Knoot's personal devices and the crimes under investigation but also fails to even establish *some connection* between the two. To hold otherwise would effectively allow law enforcement to obtain a warrant to search a suspect's devices simply because he's a suspect. And given the Supreme Court's well-known Fourth Amendment rulings highlighting the unique privacy interests implicated by device searches, *see, e.g.*, *Riley*, 573 U.S. at 373, it's difficult to see how reasonable officers could've believed that Agent Rosseau's conclusory "training and experience" allegation justified a search of Knoot's desktop and cellphone.[5]

Hoping for the opposite result, the Government, citing the Sixth Circuit's decision in *Evers*, claims that the affidavit Agent Rosseau swore out in support of the Device Warrant drew a strong enough connection between the crimes under investigation and Knoot's personal devices as to render law enforcement's act of searching those devices reasonable. (*Id.*, PageID #269).

But a careful reading of *Evers* shows that it does not help the Government's cause. There, the defendant's son—"Junior"—learned that the defendant had molested his (Junior's) thirteen-year-old cousin (the victim) and taken "photographs of her private parts." *United States v. Evers*, 669 F.3d 645, 649 (6th Cir. 2012). He further learned (from the victim) that "the photos were taken with a silver Kodak camera and [then] stored on [the defendant's] computer." *Id.* In addition, the defendant evidently told Junior that he (the defendant) had downloaded "still photos" of the victim "and her siblings" onto "his computer." *Id.* Junior evidently "opened the file" in question and "saw a movie" of the victim "that was sexually suggestive in nature." *Id.* Junior later reported this information—namely, that his father had taken sexually suggestive pictures of

[5] Along similar lines, it bears mentioning that, although the affidavit submitted in support of the Device Warrant is forty-four paragraphs long, only *eight* paragraphs—namely, paragraphs 16 through 23—contain meaningful factual content related to the crimes under investigation. (DE 50-1, ¶¶ 16-23). And, as discussed above, even a cursory review of these paragraphs reveals that *none* of them explain how Knoot's *personal* devices were used "in connection with criminal activity." *Powell*, 943 F. Supp. 2d at 779.

the victim and then downloaded those pictures onto his computer—to law enforcement. *Id.* And law enforcement, in turn, "recounted" this information "in detail" in an affidavit and then used that affidavit to obtain a warrant to search the defendant's home, along with his "[d]igital [c]amera," "[p]ersonal [c]omputer," and computer "accessories." *Id.* at 651. Upon executing the warrant, law enforcement found eighty-two images of the victim on the defendant's computer (about half of which were "sexually explicit"), and, about a month later, a grand jury indicted the defendant for producing and possessing child pornography. *Id.* at 650.

As the case developed, the defendant moved to suppress the evidence found in his house and on his computers, claiming that the warrant authorizing the search was invalid. *Id.*

But the district court denied his motion and the Sixth Circuit affirmed. Discussing good faith, the Sixth Circuit noted that, "[a]lthough the search warrant . . . was by no means a model of clarity, it cross-referenced" the supporting "affidavit, which in turn "*linked*" (with case-specific "*fact*[s]") the defendant's computer "to the offenses" under investigation. *Id.* at 654 (emphasis added). Because the affidavit drew a "link[]" between the defendant's computer and the crimes at issue—and because that "link[]" showed that the defendant's computer had been used to facilitate those crimes—the Sixth Circuit held that neither the affidavit nor the warrant were "so facially deficient" that "the executing officers could not reasonably have relied upon them." *Id.* at 654.

Here, unlike in *Evers*, the affidavit Agent Rosseau swore out in support of the Device Warrant doesn't include facts "link[ing]" Knoot's personal devices to the crimes under investigation. *Id.* Quite the contrary, such facts are noticeably absent. To that end, *Evers* does not support the Government's position that the officers in this case acted in good faith when they searched Knoot's personal devices—indeed, if anything, it supports the opposite result.

Further, this case is more analogous to cases like *Brown* and *Ramierz*—cases in which courts have *declined* to apply the good-faith exception. In *Brown*, law enforcement obtained a warrant to search a suspected drug dealer's house pursuant to an affidavit that failed to include "specific and concrete" facts linking the house to the crimes under investigation. *Brown*, 828 F.3d at 382. Because the nexus was missing, the Sixth Circuit ruled that the warrant was defective. *Id.* And because the affidavit didn't even include facts drawing a "plausible connection" between the suspected criminal activity and the suspect's residence, the Sixth Circuit ruled that "the good-faith exception [did] not apply." *Id.* at 386. Similarly, in *Ramirez*, law enforcement obtained a warrant to search a cell phone pursuant to an affidavit which (as here) stated: "Affiant knows through training and field experience that individuals may keep text messages or other electronic information stored in their cell phones which may relate them to crime and/or co-defendants/victim[s]." *United States v. Ramirez*, 180 F. Supp. 3d 491, 493 (W.D. Ky. 2016). Citing *Schultz*, the district court concluded that this allegation was insufficient to authorize a valid search of the cellphone. *Id.* at 495-96. And then, as to good faith, it said: "An objectively reasonable law enforcement officer would have recognized that this affidavit was so lacking in indicia of probable cause as to preclude good faith reliance on the search warrant." *Id.* at 496.

The same is true here. Any reasonable person reading the factual portion of the warrant affidavit (i.e., ¶ 16 through ¶ 23) would conclude that the victim laptops were instrumentalities of crime and, therefore, subject to search and seizure. But nothing in this factual portion makes even a passing reference to any devices *other* than those laptops—such as, for instance, Knoot's personal computer and cellphone. Rather *those* devices are only connected to the case because Agent Rosseau vaguely said that his "training and experience" has taught him that "[i]ndividuals who engage in criminal activity" use digital devices to do so. (DE 50-1, ¶ 26).

Because "[a]n objectively reasonable law enforcement officer would have recognized that" allegation was insufficient to draw a case-specific link between Knoot's devices and the crimes under investigation, *see Ramirez*, 180 F. Supp. 3d at 496, the good faith exception does not apply.

And since an objectively reasonable officer would have recognized that he had no business searching Knoot's personal devices, such an officer also would have realized that he could not use information obtained from those devices to compel Discord to produce certain communications. *Smith*, 730 F.2d at 1056 (providing that, when "tainted information [is] so important" to the warrant affidavit that the warrant would not have been issued without it, suppression is warranted).

CONCLUSION

In sum, the Government seized and searched Knoot's personal desktop computer and cellphone pursuant to a defective warrant and then used information discovered on that desktop and cellphone to compel Discord, Inc. to disclose (to the Government) communications between his Discord account ("mellamomateao") and another Discord user (username "yandgi0027").

Under these circumstances, this Court should—at the very least—suppress: (1) any information law enforcement obtained from Knoot's personal devices (i.e., his personal desktop computer and cellphone), and (2) the Discord communications between "mellamomateao" and "yandgi0027" (because the Government used tainted information to obtain them).

Respectfully submitted,

s/ *David Fletcher*
DAVID FLETCHER
Assistant Federal Public Defender
810 Broadway, Suite 200
Nashville, Tennessee 37203
615-695-6951
David_fletcher@fd.org

Attorney for Matthew Knoot

CERTIFICATE OF SERVICE

I hereby certify that on April 28, 2025, I electronically filed the foregoing *Reply in Support of Motion to Suppress* with the U.S. District Court Clerk by using the CM/ECF system, which will send a Notice of Electronic Filing to the following: Josh Kurtzman, Assistant United States Attorney, 719 Church Street, Suite 3300, Nashville, Tennessee, 37203